NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

IMPLICATIONS OF USER IDENTIFICATION DEVICES (UIDS) FOR THE UNITED STATES NAVY

by

Letitia D. Haynes

September 2001

Thesis Advisor:	Cynthia Irvine
Associate Advisors:	Tim Levin
	Floyd Brock

Approved for public release; distribution is unlimited

Report Documentation Page

Report Date 30 Sep 2001	Report Type N/A	Dates Covered (from... to) -

Title and Subtitle		Contract Number
Implications of User Identification Devices (UIDs) for the United States Navy		Grant Number
		Program Element Number

Author(s)	Project Number
Letitia D. Haynes	Task Number
	Work Unit Number

Performing Organization Name(s) and Address(es)	Performing Organization Report Number
Research Office Naval Postgraduate School Monterey, Ca 93943-5138	

Sponsoring/Monitoring Agency Name(s) and Address(es)	Sponsor/Monitor's Acronym(s)
	Sponsor/Monitor's Report Number(s)

Distribution/Availability Statement
Approved for public release, distribution unlimited

Supplementary Notes

Abstract

Subject Terms

Report Classification unclassified	Classification of this page unclassified
Classification of Abstract unclassified	Limitation of Abstract UU

Number of Pages
72

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY (*Leave blank*)	2. REPORT DATE September 2001	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE: Implications of User Identification Devices (UIDs) for the United States Navy		5. FUNDING NUMBERS	
6. AUTHOR(S) Letitia D. Haynes			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		10. SPONSORING / MONITORING AGENCY REPORT NUMBER	

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	12b. DISTRIBUTION CODE

13. ABSTRACT (*maximum 200 words*)

Various technologies are emerging to provide enhanced, automated personnel identification capabilities. Techniques for human microchip implants using radio frequency identification are possible, but the implications of this technology remain to be considered. This thesis provides a survey of current technologies for enhanced user identification, focusing on human implant approaches, and to summarize the set of security, privacy, social and ethical issues that may arise from the use of these technologies in the U.S. Navy. Technical background is presented to provide the reader with a basic understanding of radio frequency technology. An analysis of human implant technologies currently used in the private sector is provided to show how they might offer capabilities in the military. Applications of information technology and human microchip implants that may improve user identification in the future are presented and analyzed. Finally, a review of the social and ethical implications of human implant-based user identification is provided. It shows that the collateral social issues are complex and far-reaching, and need to be carefully considered by the Navy to avoid becoming entangled in intractable technical, morale and legal issues far into the future. The results of this exploratory thesis show: 1) implementation of advanced information technology devices must be carefully balanced against human social and ethical considerations, and 2) there is a valid need for future research and analysis of human microchip implants.

14. SUBJECT TERMS: User Identification Devices, Human Microchip Implants, Ethics, Security, GPS, Military Operational Medicine			15. NUMBER OF PAGES 72
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

IMPLICATIONS OF USER IDENTIFICATION DEVICES (UIDS) FOR THE UNITED STATES NAVY

Letitia D. Haynes
Lieutenant Commander, United States Navy
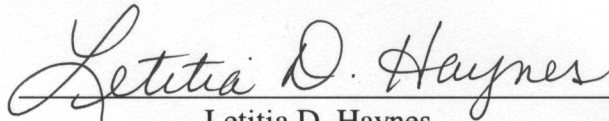B.S., University of Central Florida, 1987

Submitted in partial fulfillment of the
requirements for the degree of
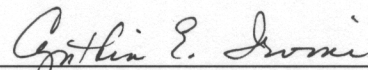
MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the
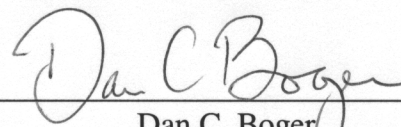
NAVAL POSTGRADUATE SCHOOL
September 2001

Author: _____
Letitia D. Haynes

Approved by: _____
Cynthia Irvine, Thesis Advisor

_____
Tim Levin, Associate Advisor

_____
Floyd Brock, Associate Advisor

_____
Dan C. Boger
Information Systems Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Various technologies are emerging to provide enhanced, automated personnel identification capabilities. Techniques for human microchip implants using radio frequency identification are possible, but the implications of this technology remain to be considered. This thesis provides a survey of current technologies for enhanced user identification, focusing on human implant approaches, and to summarize the set of security, privacy, social and ethical issues that may arise from the use of these technologies in the U.S. Navy. Technical background is presented to provide the reader with a basic understanding of radio frequency technology. An analysis of human implant technologies currently used in the private sector is provided to show how they might offer capabilities in the military. Applications of information technology and human microchip implants that may improve user identification in the future are presented and analyzed. Finally, a review of the social and ethical implications of human implant-based user identification is provided. It shows that the collateral social issues are complex and far-reaching, and need to be carefully considered by the Navy to avoid becoming entangled in intractable technical, morale and legal issues far into the future. The results of this exploratory thesis show: 1) implementation of advanced information technology devices must be carefully balanced against human social and ethical considerations, and 2) there is a valid need for future research and analysis of human microchip implants.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS

AAPS	Association of American Physicians and Surgeons
AIDC	Automatic Identification and Data Capture
ASR	Artificial Silicon Retina
BMO	Biometric Management Office
DOD	Department of Defense
DON	Department of Navy
FDA	Food and Drug Administration
GBS	Global Broadcast Service
GPS	Global Positioning System
IDM	Information Dissemination Management
IEEE	Institute of Electrical and Electronic Engineers
Mbps	Megabits per second
MBS	Modulated Back Scattering
MIT	Massachusetts Institute of Technology
NSC	Naval Space Command
PAN	Personal Area Network
PDA	Personal Digital Assistant
PLC	Programmable Logic Controller
POS	Personal Operating Space
RFID	Radio Frequency Identification
SBS	Southern Biosystems
TG	Task Group
UIDs	User Identification Devices
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

And finally, I would like to thank my family; my mother Dorothy White for instilling my desire to succeed, to my husband Greg, whose unwavering support I appreciate, and a special little thank you to my son Miles T. Jubert who always reminded me to maintain the delicate balance of life: have faith in God, work hard, do well in school and of course don't forget about "my" soccer games. Thank you Miles, it was your smile that kept me going.

I. INTRODUCTION

A. BACKGROUND

User identification is becoming increasingly more important in our era of information technology. Both private and governmental bodies are making efforts to refine and improve the identification processes and devices. Included in the search for perfecting the identification process is the desire to make it convenient as well as secure. For example, it is important to ensure that the right individuals are given access to the intended information or specified area. Although many private entities are more flexible in their ability to test and implement new user identification procedures, government entities are not as fortunate. In the private sector it appears to be a race as to whom can provide an identification system that provides a fast, secure, and error free system. [TIRF00] As considerations are being applied to new realms of technology to make life more convenient and secure, implications of these new technologies should be analyzed. Our society is making great efforts and progress in the direction of user identification, such as biometrics and smart technologies. However this thesis goes beyond biometrics and smart technologies. It takes you, the reader, to a new realm of technology. Can human microchip implants offer a better or improved or even a secure way of accessing information? Where, for example, the identification is absolute and we know beyond any doubt who is requesting and who is receiving the information. While some devices come close, others fall short of the intended desires or needs of the user. Our society is realizing that while we strive to gain advanced technologies in this information age, we also struggle with the ethical and social implications that these technologies bring about. We are learning that major implications must be considered prior to implementing a new and challenging concept or technology.

B. OBJECTIVE

The purpose of this thesis is to explore the emerging technologies that affect user identification. The conclusions may not be a popular recommendation or politically correct, yet they constitute a careful analysis of current information.

The goal is to assist the reader by describing in laymen's terms technological capabilities in the civilian sector and how they might be used in the military.

1

C. SCOPE AND METHODOLOGY

The scope of this thesis research is to identify automatic processes and devices for user identification, explain the technology of radio frequency identification and its application, present potential uses of this technology, and offer some initial intangible implications.

The methodology used in this thesis research consisted of an extensive search and review of periodicals, available books, the Internet, and World Wide Web resources. The personal interviews conducted by phone, email, and office visits were especially helpful, particularly the interview with Dr. Frank Kocher, a local veterinarian. This allowed for an up close, firsthand demonstration of the latest technology. An unimpeded and candid interview with a staff nurse at a local hospital offered a peek into how this technology is being used in the hospital. A few requests for interviews were refused or ignored, which allowed the author to understand the public sensitivity to the information sought.

The author's curiosity in this subject matter began early on while attending a space systems class in the spring 2000. A review of a listing of potential thesis topics posed by Naval Space Command (NSC), gave rise to a quest to learn more about embedded identification schemes such as microchip implants. I made contact with the individual responsible for suggesting this topic at NSC, Emmett Henderson. The resulting conversation stimulated my interest and research into the applications of microchip implants.

Often the military is an organization that has lived and died by the sophistication of physical weaponry on battlefields. The way we defend our country, fight our battles, and the future of the battlefield is changing. Computer and information technology is playing a larger and more integrated role than it ever has before. Will the future of the military be significantly dependent upon these interlocking technologies? It is evident that the U.S. military is becoming vastly more dependent upon the convergence of computer science and information technologies.

D. ORGANIZATION OF THE THESIS

The thesis is organized into six chapters. This chapter provides the introduction, objective, scope and methodology used to conduct the research. Chapter II provides a

background on the automatic data capture and gives a foundation of radio frequency technology as a basis for understanding wireless microchip technology used in inanimate objects and in animals. Chapter III identifies the uses of radio frequency technologies, areas of various applications. Chapter IV identifies potential uses and scenarios for the application of user identification devices for the U.S. Navy and private sector. Chapter V presents the social considerations associated with human microchip implants. Chapter VI covers conclusions and future considerations as derived from this thesis exploration.

THIS PAGE INTENTIONALLY LEFT BLANK

II. AUTOMATIC IDENTIFICATION AND DATA CAPTURE TECHNOLOGY (AIDC)

This chapter presents an introduction to automatic capture of data for purposes of user identification. A few of the latest technologies that are being implemented in the Department of Defense (DoD) are briefly explained. A basic introduction of radio frequency identification is presented and offers a prelude to the various applications of this technology that is presented later.

A. DEFINITION OF USER IDENTIFICATION DEVICES (UIDS)

User Identification Devices (UIDs) in this forum are used to describe a tangible object or a process that detects the characteristic(s) of the consumer(s) or producer(s), and attempts to uniquely classify that entity. The objective of UIDs usually is to maintain access control and accountability. Currently our business environment supports many UIDs, and there are continuing efforts to make them smaller, more convenient, easier to transport and maintain, and more efficient with regard to data throughput. More importantly, desires to enhance the security and integrity of UIDs is at the forefront. Many UIDs are currently in operation. There are plastic badges or cards that use a combination of pictures, barcodes, magnetic strips, embedded microchips (called smart cards), biometrics, and passwords. Among the latest identification technologies being advanced are the use of radio frequency, noncontact transmission methods to be expounded upon later, and microchips. The objective of these efforts is to automatically capture data for accurate identification and greater spatial range of decision making.

B. AUTOMATIC IDENTIFICATION AND DATA CAPTURE (AIDC)

"Automatic Identification and Data Capture (AIDC) is the worldwide industry term which describes the identification and/or direct collection of data into a computer system, programmable logic controller (PLC), or other microprocessor-controlled device without using a keyboard." [AIM00]. This capability of identifying and accessing data in secured areas within the business world and without the use of keyboards has lead to the use of contact and noncontact badges and cards.

1.   Smart Card Technology

"The first plastic cards appeared in the USA as early as the beginning of the 1950's with the introduction of plastic credit cards; the first one being issued by Diners Club in 1950" [FINK99, p. 227]. Technological advancements soon followed in the area of integrated circuitry. This made it first possible to integrate data memory and processing logic onto a single silicon chip. The desire for the convenience of a smaller transaction tool caused the two to merge into what is known as the "smart card." The smart card device is a form of UID that closely resembles a plastic credit card but possesses an embedded microchip. A microchip is an integrated circuit that can process and store data, which usually resides on the front of the card between two layers of plastic. A technical committee of the International Organization for Standards (ISO) sets forth the dimensional and other device standards. For instance, noncontact[1] smart cards are governed by ISO 10536. [FINK99, p. 163]

Today the market demand for smart cards is growing rapidly, as indicated by a three-fold increase in their worldwide issuance from 1992 to 1995: from 200 million to 600 million. [FINK99, pp. 4-5] These smart cards were first used to support prepaid telephone cards in 1984 [FINK99, p. 5]. American Express Blue then became the first credit card in the United States with a microchip in September 1999 [AMEX]. Soon other major credit cards followed suit.

Now that plastic card design and microchip technology have been combined, serious consideration is being given to the merger between smart card technologies and biometric identification. For example, many state motor vehicle departments are digitizing an individual's driver's license photos on the driver's license card. Also, fingerprints have been digitalized, and a picture copy of the fingerprint placed on a card. [BOWE94, p. 58] Now it is likely for one's fingerprints or signatures to be digitalized and stored on a microchip and further housed on a card. Biometric technology is being touted as an accurate and automated means of identifying individuals. The following section will further define and discuss biometric technology.

---

[1] Briefly contact cards are those cards that require physical contact with a reader device and noncontact cards are those cards that do not require physical contact with a reader device.

2.   Biometric Technology

Biometric technology is the use of human bodily characteristics or "physiological autographs" [GARF00, p. 41] in an attempt to uniquely and absolutely identify individuals. The earlier forms of unique body characteristics were recognized in the science of fingerprints in the 1970's.   In the 1980's, the Automated Fingerprint Identification System (AFIS), developed by NEC Technologies completely changed the role of fingerprints. It combined computer graphics with special software programs and parallel processing to create forensic results. [GARF00, p. 45].

Today biometric technologies include retina prints, iris prints, signature and handwriting analysis, palm prints and hand geometry, voiceprints, face recognition, facial thermograms, silhouette identification and gait prints, and even specific task performance and writing styles. [GARF00, pp. 56-59].   Of all the aforementioned biometric identification systems, iris prints appear to be the most accurate. The iris patterns of each person's eyes are fixed before birth and remain unchanged throughout one's life unless trauma interferes. It is important to note that all of these forms of biometric identification do not uniquely identify the individual; instead, the unique body scan identifies that particular body part or characteristic. Linking the name with the body scan "requires looking up the scan in a computerized database," which in turn opens itself up to security vulnerabilities. [GARF00, p. 57]

Biometrics is widely used in fields as varied as e-commerce, network access, time and attendance, ATM's, corrections, banking, and medical record access. [BIOG] Due to the apparent ease of use, and other factors, biometric technology applications are being used increasingly throughout private businesses, and governmental sectors. Even the Department of Defense is looking "beyond passwords" to provide the best reliable and available security access systems" by having established a central control coordinating government office, called Biometric Management Office (BMO). [BMO] This newly established organization will be discussed more fully in section D of this chapter.

Although phenomenal growth in both smart card and biometric technologies has been witnessed, another area of more recent and rapid growth is the merging of these and many other technical elements into the field of Radio Frequency Identification (RFID).

C.   RADIO FREQUENCY IDENTIFICATION (RFID) TECHNOLOGY

As evidenced by market sales, Radio Frequency Identification is one of the fastest growing sectors of radio technology, and this includes all mobile and cordless telecommunication devices. "Total worldwide sales of RFID systems for the year 2000 have been estimated at over 2 billion U.S. dollars." [FINK00, p. 1]

1.   Definition of RFID

Radio Frequency Identification (RFID) has been used for automatic data collection since World War II. More recent applications include toll road management, asset management, identification and control, and most aggressively animal identification and human assistance and support. [TUTT97]

Radio Frequency Identification has proven to be more useful than the traditional bar code technology, such as grocery store scanners; because RFID it does not use light transmissions and can "sense" or detect the remote device through almost any barrier and in most inclement or data challenged environments.

Radio Frequency Identification uses electromagnetic energy to communicate within its system. A very basic RFID system discussed in this paper is composed of the following components: a microchip and a scanner or reader. There are two different classes of transponder devices that house the microchip: passive and active.

a.   *Passive Devices*

Passive devices are those that do not have any energy or power of their own. The device is completely dormant and relies upon the scanner to come within a certain distance to "activate" it. Hence, its power is derived from the radio frequency energy transmitted from the reader. The majority of these remote devices are being made smaller and more compact than their predecessors. Today, microchips are small enough to be implanted in the animal population, which will be discussed at length in Chapter III. In those cases, the dimensions of the microchips are about 11 mm by 2.1 mm. They weigh about 0.06g or 0.002 oz., and have an operating frequency of 125kHz, which is a low frequency range. (ELEC01) Once the passive device is activated, it reflects energy and is able to transmit its housed data to the radio frequency scanner using modulated backscatter (MBS) [TUTT97]. "In relation to passive devices, an interrogator (reader) transmits an unmodulated carrier. The transponder senses this and varies the reflective

properties of its receive antenna so that it reflects the unmodulated carrier or absorbs it. Possibly the interrogator (reader) acts like a radar, waiting to receive returns from any target (transponder) within its sensing range. In this case, the transponder reflects/does not reflect in a pattern related to its identification number." [IVES01, MBMS] In this case, an example provided by Dr. Robert Ives, a pattern like: reflect-reflect-reflect- not reflect-not reflect-reflect = 1 1 1 0 0 1. See Figure 1 which diagrams the basic process for a passive device, and see Figure 2 for a more detailed diagram of a passive device.
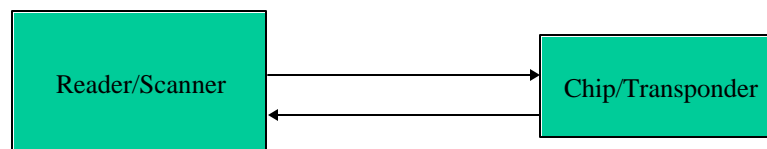
Basic process of passive transponder:
1. Transponder is dormant and gives no signal or information
2. Reader comes within specified range of transponder
3. Activation is caused by the reader signalling to the transponder
4. The transponder "awakens" and sends a response, which is the
    data that resides on it

Figure 1.   Basic Process for Passive Device, Depicted by Author.

Use of modulated backscatter (MBS) is better where there are very few obstructions in the energy path, the distance is (under six inches), and where there is no chance of detecting other identification devices, that would cause collisions and confusion. [TUTT97]
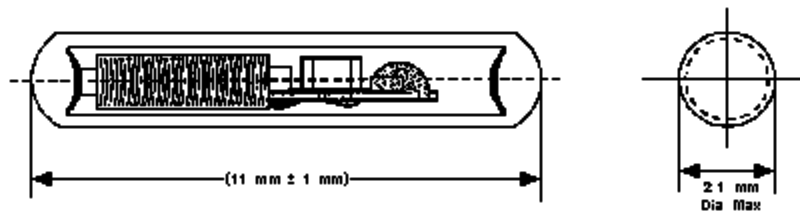
Dimensions (nominal): 11 mm by 2.1 mm (0.43" by 0.08")
Housing: Bio-compatible glass
Average weight: 0.06 g (0.002 ounces).
Temperature range: -40 to 70'C (-40 to 158'F), operating and storage
Read range with the HS5105L Mini-Portable Reader:
(in a benign noise environment with optimal orientation of transponder and scanner)
Maximum: 1 0 cm (4")
Vibration:
Sinusoidal; 1.5 mm (0.06") peak-to-peak, 1 0 to 80 Hz, 3 axis
Sinusoidal; 1 0 g peak-to-peak, 80 Hz to 2 kHz, 3 axis
Injector needle size: About 12 gauge
Operating frequency: 125kHz

Figure 2.   Example of Passive Device, "Implantable Transponder TX1400L" from
Electronic ID, Inc., http://www.electronicidinc.com/tx14001.html.

b.   *Active Devices*

Active devices are usually larger in size, have longer-range capabilities, have their own power source (batteries), and do not rely upon the scanner to activate their capabilities. Some active RFID devices offer read-write options. Due to their self-containment, active RFID devices are used in applications where there is no line of sight from the scanner to the remote device, significant obstructions, are in place, or a longer range is required. It is important to note that the longer the distance, the higher the required frequency to get a "reading" output from the source. Thus, the remote device must use more power to transmit back to the requesting source (scanner). This, in turn, affects the design of the antenna at the source. The more efficient the antenna designs, the better the quality of the return data. Figure 3 is a diagram of the Digital Angel System Architecture, which uses an active microchip in a wearable device on humans and on animals. Digital Angel will be described in more detail in Chapter III.

Digital Angel™ *System Architecture*
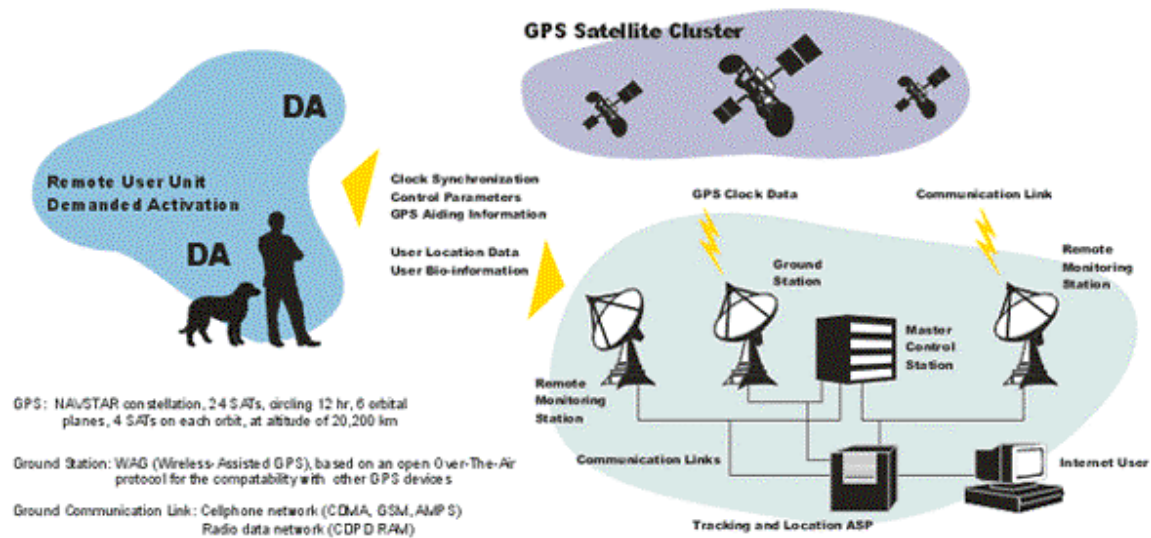
Figure 3.   Digital Angel System Architecture; Shows Example of an Active Device in Use. (Source: "The Technology Behind Digital Angel" http://www.digitalangel.net/da/tech.htm.

2.   Overview of Applications and Trends

There are many application areas of RFID in use today. Some of the more intriguing areas that more closely affect end users are mentioned in detail in the following chapter. Now, however, a brief overview of typical applications is presented. RFID is being used in the following environments: public and ticketing transport systems, electronic container identification, and industrial automation. The American Express Blue card offers a reader device to enable the user to make online purchases from a home PC more securely. [AMEX] RFID is also being used in sporting events. For example, when a sprinter finishes his or her race, the speed can be timed through a transponder placed on his or her shoe and noted by the equipment at the finish line through RFID technology. This information can be fed almost simultaneously to the announcer at the event. [FINK99, pp. 229 & 263]

By combining RFID with satellite technology, another element can be introduced. This is the capability of trackable identification devices. As can be expected, this type of identification conjures criticism and scrutiny within our society concerning ethical and privacy issues. The more specific technical applications will be discussed in Chapter III,

11

and Chapter IV discusses the social aspects that must be considered. Both aspects of this technology greatly affect the general public.

D. DEPARTMENT OF DEFENSE BIOMETRIC MANAGEMENT OFFICE (BMO)

The Department of Defense (DOD) has begun to update their technology in the user identification sector. Recently the DOD announced the opening of a new office and entity called the Biometrics Management Office. The Department of the Army was designated as DOD's Executive Agent for developing and implementing biometric technology. [BMO01]

The overall mission of the Biometrics Management Office (BMO) is to ensure the availability of biometrics technologies within the DOD. Specifically the Army Chief Information Officer, acting on behave of the Secretary of the Army ensures the BMO operates as the executive agent to lead, consolidate, and coordinate all biometrics information assurance programs of the DOD in support of Network Centric Warfare.

> The BMO manages a full spectrum of biometrics systems and technologies that are focused on providing Soldiers, Sailors, Airmen, and Marines with a technological edge in all environments by providing proven, reliable, and effective biometrics access systems in support of garrison and combat operations. [BMO01]

As described in their vision statement, BMO will strive to provide the DOD user an edge in all operational environments with the best reliable and available security access system. [BMO01] The Department of Defense BMO is searching for absolute user identification devices, in an attempt to improve upon DOD's outdated identification technology.

E. COMMON ACCESS CARDS

The Department of Navy (DON) is on a mission to distribute 800,000 common access cards by September 30, 2002. The DON is currently issuing more than 1000 cards each work day, and few speculate that their goal is overly ambitious. "These cards are being issued to active-duty service members and civilian defense employees, as well as some reservists and contractors. Beyond controlling access to buildings, computer networks and web servers, these cards will hold basic identification data on a microchip." [MURR01]

On May 19, 2000 General Services Administration (GSA) announced contract awardees of its government-wide Smart Access Common ID contracts to five prime companies all located in Northern Virginia. The contracts are worth a maximum value of $1.5 billion over 10 years and have a base period of two years, with two four-year extension periods. The Commissioner of GSA's Federal Technology Services, Sandra Bates, anticipates that these cards will greatly enhance the security of government facilities and systems on a worldwide basis. She says they will use chip card technology and support many important applications to provide for interoperability. [GSAA00]

The Department of Defense's Biometrics project and the Department of Navy's Common Access Cards project are two new and different user identification schemes. These large projects are being promoted and implemented within the government. It would be beneficial if both projects have compatible infrastructures so that more efficient operations can take place, maybe even combining the two technologies into one.

THIS PAGE INTENTIONALLY LEFT BLANK

III. RADIO FREQUENCY IDENTIFICATION APPLICATIONS

This chapter reviews some of the latest technological applications in radio frequency identification as well as applications that relate to implants. The social and ethical concerns arising from the use of these technologies will be addressed in the Chapter V.

A. WIRELESS PERSONAL AREA NETWORKS (WPANS)

1. Electrical Body Communications

Thomas G. Zimmerman, a graduate of Massachusetts Institute of Technology (MIT), completed master's thesis work in 1995 that "introduced the new concept of a personal area network (PAN), a wireless communication system that allows electronic devices on and near the human body to exchange digital information through near-field electrostatic coupling, developed by Neil Gershenfeld." [ZIMM95, p. 8] Due to the increasing number of electronic devices that are carried or worn on a person, i.e., a watch, pager, cellular phone, personal digital assistant and laptop computer, a need was recognized for the capability for all of them to exchange data and reduce the duplicity of similar hardware. This interoperability was the motivation for his research, which also lead to experiments and the development a working prototypical PAN. In his experiment, two people who wore PAN devices were able to exchange electronic business cards by shaking hands (causing capacitive coupling, providing a non-radiating signal). The physical act of shaking hands caused an external transmitter worn by one person (that contained ASCII characters stored in a memory program) to transmit the data to a receiver attached to the other person. When the receiver obtained the data, it was demodulated and sent to a host computer. [ZIMM95, p. 57] After his work, more studies in PAN began as industry concerns and interest increased regarding common network structures for personal wireless devices.

2. Personal Operating Space

On March 12, 1998 the IEEE organization created the Wireless Personal Area Networks (WPAN) Study Group. This study group was created to investigate the need for a supplemental wireless network standard. Specifically the study group's focus was targeted to provide a simple, low complexity wireless connectivity environment for

personal devices within or entering a Personal Operating Space (POS). [IEEE00] The IEEE has defined POS as the space about a person that typically extends up to 10 meters in all directions and envelops the person whether stationary or in motion. Emerging from this study group was the IEEE 802.15 Working Group for WPANs[2] whose goal is to achieve interoperability, which would allow the transfer of data between a WPAN device and an 802.11 device (WLAN device). Today the IEEE 802.15 Working Group develops Personal Area Network consensus standards for short distance wireless networks, also known as WPANs[TM3]. They have several task groups working on the following projects: TG1-WPAN/Bluetooth, TG2-Coexistence Mechanisms, TG3- WPAN High Rate (20Mbps or greater) and TG4- WPAN Low Rate. The IEEE 802.15 TaskGroup 4 is chartered to investigate low data rate technologies each with multi-month to multi-year battery life and low complexity. "It is intended to operate in an unlicensed, international frequency band. Potential applications are sensors, interactive toys, smart badges, remote controls, and home automation." [IETG4]

B.   COMMERCIAL USE OF RADIO FREQUENCY IDENTIFICATION

There are numerous commercial applications of radio frequency identification, many that touch our lives almost daily. As more products continue to enter the commercial markets, so does our seemingly unintentional dependency upon them. Ubiquitous computing and technology systems are becoming more prevalent in our society. Our nation currently uses radio frequency technology in such environments as asset management and control, electronic toll collection and traffic management, and law enforcement (parolee tracking, and electronic surveillance), the latter of which is of particular concern to the general public.

An innovative new use of radio frequency identification is for tracking of newborns in hospitals. Within minutes of a baby's birth, he or she is checked and cleaned; and an identification device is attached to the leg of the infant so as to deter kidnap and/or misidentification. This device is a small plastic box approximately 1 inch x 1 inch in size. It is placed on the infant's leg and the information housed within has his

---

[2] WLAN is industry wide term for Wireless Local Area Network.

[3] WPAN is a trademark of IEEE, Digital Angel (presented in section C.2) is a trademark of Applied Digital Solutions. BioBond is a trademark of Destron Fearing (presented in section D.1) owns the patent.

or her surname and room number. The attending nurse only has a few seconds to attach, adjust and secure the device to the newborn's leg before the device is activated and identifies the baby. Companion devices detect the infants' devices through a wireless medium (radio frequency) and are located throughout the maternity ward (within each room, in the hallways and near the nurses station). Afterwards, if anyone carries the baby too far from the designated areas in the maternity unit, an alarm is sounded and the hospital staff begins a plan of action. [CHOM01]. More medical technological advances in regards to microchip implants are discussed in the section D.

C.   WEARABLE DEVICES

Wearable devices are becoming a popular. The target markets are from businesses that require personnel to wear them to assist in their job responsibilities, monitoring athletes and high performers, to the everyday person. A few will be briefly described in the next section.

1.   Smart Clothing

Researchers in the area of electronic technology are teaming up with fabric and fashion designers to produce high-performance fabrics that will ultimately combine electronic devices to enhance fashion as well as function. Recently a "smart" space suit outfitted with wearable computers was tested in Russia. The suit, built in collaboration with Boeing Company, is designed to monitor an astronaut's condition while providing information and feedback during space walks outside the space station. The research piece of clothing is called the "smart vest." It is an undergarment made with flexible conductive fibers that could be used as a kind of motherboard for connection of wearable devices. [WSJ01, p. B3]

Sensatex Inc., a technology start-up company, is focusing their efforts in the fitness arena. They are refining a "smart shirt" prototype after obtaining an exclusive license to technology developed at Georgia Institute of Technology for monitoring battlefield soldiers. This prototype mimics a soft, cotton knit T-shirt; but the cotton and spandex cloth is interwoven with conductive fibers that can receive and transmit data from embedded sensors to a special receiver the size of a credit card. It is intended for the receiver to be worn at the waist and store information that can be played back to a

cellular phone, home personal computer or a wrist-mounted monitor. The company is expecting to vend its finalized shirt product for about $200. [WSJ01, p. B3]

2. Federal Express and Texas Instruments RFID

FedEx couriers have one less thing to keep track of these days—their vehicle keys. The company's couriers use an automatic keyless entry and ignition system that has RFID transponders embedded within a Velcro wristband. This technology is being provided to Federal Express by Texas Instruments. The system is being tested in 200 FedEx delivery vehicles.

With RFID, FedEx delivery personnel are freed from the hassles of juggling their keys while carrying armloads of packages and are more productive along their routes. If a wristband is misplaced, its code can be purged from the system; and a new code can be reprogrammed in a matter of seconds. [TRIF00]

Cases where delivery personnel have misplaced their keys and then had to wait for replacements was costing Federal Express more than $200 per incident. [TRIF00]

3. Digital Angel™

One of the most talked about new radio frequency identification devices is Digital Angel, made by Applied Digital Solutions (ADS) Digital Angel is designed to be worn close to the body to monitor the whereabouts of a person and monitor their designated body functions. The company is currently taking preorders, through their web site, for its pending release in October and December 2001. The cost is approximately $299. The device is being marketed to the caretakers of children and to elderly adults. In addition, they are also marketing a Digital Angel Pet System, which is collar based. The company's plans are to make it available in January 2002. The human wearable products take on one of two forms: a wristband watch or a pager device. These products utilize microchip-based Code-Division Multiple Access (CDMA) technology. CDMA is a digital cellular technology that uses spread-spectrum techniques. Specifically it uses Cellular Digital Packet Data (CDPD) operating at 900MHZ and has Global Positioning System (GPS) capability to receive at 1.5GHz. [ARKI01]

The Digital Angel prototype made its first public demonstration debut in New York City in October 2000. It is publicized as being the "first-ever Operational combination of advanced sensor technology and Web-enabled wireless telecommunications linked to GPS satellite systems." [ADS00] News about Digital

Angel was publicly released in September 2000; and interest has since been expanding rapidly. On September 11, 2000 Applied Digital solutions announced the merger of their subsidiary Digital Angel.net Inc. with Destron Fearing Corporation, one of the leading manufacturers of microchip implants for animals. Then on February 11, 2001, they announced the "formation of a strategic alliance with AT&T Wireless as its wireless carrier of choice for the Digital Angel Delivery System." [ADS01]

It is worth noting that these strategic business mergers and alliances bring closer the possibility of a transition in the use of microchip implants from the animal population to the human population. It could be only a matter of time before this company (ADS), that has merged two technical advanced but distinct business units (wearable tracking and monitoring devices for humans and animal identification devices), announces unimaginable and complex applications. Due to their business foresight and the upscale trends in technology developments, this company is worth following closely.

The next section will present a more detailed observation of microchip implants in the animal population and limited specific applications within the human population.

D.   MICROCHIP IMPLANTS

1.   Animal Population Control & Identification

Currently passive microchip devices are being used in a wide variety of "wildlife" animals or domesticated pets. There are said to be over 4 million microchips implanted in animals, with a capacity for over 70 trillion possible microchip identification codes. [IMT00] Many city governments are now mandating a microchip identification program within their responsible Animal Control Departments. While some cities have assumed this task voluntarily starting in about 1996, the State of California is considering passing a bill that will make it mandatory that animal shelters that pick up stray domestic pets incorporate them into the microchip identification program. Back in 1996, the City of Los Angeles selected InfoPet Identification Systems and Troval technologies for pet identification in city shelters. [RFID96] Prior to the mandatory process of implanting microchips into stray animals, the animal shelters had no assured way of determining if a found pet had a microchip implanted or not. This was largely due to newness of the animal microchip identification program, when various manufacturers' scanners were not compatible or interoperable. Today, after a few years of political hearings and

discussions, it is possible for all microchip readers to scan an animal that has any brand microchip. Once the microchip is scanned, the reader reveals at the least the microchip brand name. In cases where a microchip is the same brand as the reader, the scanner reveals the name of the manufacturer and its 9 to 10 digit factory-installed identification. This solution came about after it was unfortunately revealed that animals would be put to sleep with the assumption that it had no microchip implant, when in fact the animal did, but the scanner could not decipher another company's microchip. [AVID]

Domestic pet owners can voluntarily have a microchip implanted in their cat or dog at prices ranging from $20 and up. The passive microchip is usually implanted in the back of the animal between the shoulder blades (scruff, back of neck). In the case of domestic animals, these microchips come preassembled from the manufacturer. The administrative instrument can be a 12-gauge syringe or sterile injector that already has the prenumbered microchip within its chamber. This system is designed for single, one time use; therefore each administration instrument is individually wrapped and properly discarded afterward as required. Some companies offer a collar tag (HomeAgain) as an extra measure, which is preprinted with the AKC Recovery Service telephone number and the microchip's unique identification code (This tag is optional and comes with a $5-$6 additional fee).   The animal microchip implant is a simple procedure in the veterinarian's office (in cases of domestic pets) and does not require the administration of anesthesia. [KOCH01]

Figure 4.   AVID Microchip from Dr. Frank Kocher's Office, Pacific Grove, CA.

Once the microchip is implanted into the animal, it should remain in place for the remainder of the animal's life. The microchip is encapsulated in a special anti-migration material. In the case of the company Destron-Fearing, their microchips are encapsulated

with a patented BioBond™ anti-migration cap that is a porous polypropylene polymer sheath. The use of this material and the like are intended for increased retention by promoting the development of fibrocystic and collagen fibers around the implant, thus inhibiting movement of the implant from its intended location. [DEST]

This author had a unique opportunity to visit and interview a local veterinarian, Dr. Frank Kocher of Pacific Grove, CA. During the interview, Dr. Kocher discussed his experience with the domestic animal identification system. This opportunity also allowed for some pictures to be taken, Figure 4 displays a comparison of a microchip to that of penny. His few years of experience with administrating the microchips to pets have been positive. Only on one occasion has he experienced a pet owner's return of her dog after it had the microchip implanted. Upon examination it was revealed that the microchip had migrated to the dog's foot. In this case, there was no desire or recommendation for removal but instead the owner chose to have another microchip implanted. During the visit, the author was offered the opportunity for a first hand observation of a prepackaged and fully sealed implantation administration instrument. It's chamber housed a prenumbered microchip. It was observed that the scanner had to be within roughly 4 inches to 6 inches before it detected the implanted device (AVID product with nine-digit identification number).

There are quite a few local and state databases that house information for recovery and reuniting pet and pet owner. PETtrac owns and operates a worldwide pet registry, and their main central databank is located in Norco, California. Also, on the increase are a number of animal shelters that have their own database with the same information as well. For example the HomeAgain Microchip Identification System requires that each 10-digit microchip code be registered with an American Kennel Club's (AKC) Companion Animal Recovery Program. In these registry programs, the pet owner completes an enrollment form containing information such as follows:

- Name of Pet Owner
- Address of Pet Owner
- Telephone number/fax number of pet owner
- Same information for alternate person to contact

- Same information for the Veterinarian/Implanter
- Pet information: name, breed, gender, date of birth, weight, color and markings, medication and other important data
- Microchip identification number used

Once a lost pet is found and the HomeAgain microchip is identified inside the animal, the shelter will contact Companion Animal recovery, which will, in turn, contact the pet's owner or, if necessary, whomever else was identified on the enrollment form (veterinarian, relative or friend). Companion Animal Recovery personnel maintain the central database 24 hours a day 365 days a year. The next section discusses a few uses of implants (electronic and microchip) within the medical field.

2. Several Medical Advances

A great many technological advances have been made in the medical use of microchip products. People in need of cures for diseases and ailments have always been willing to try new products, procedures, or processes to reverse or cure their physical afflictions.

a. Retina Chip

The U.S. Food and Drug Administration (USFDA) in early 2000 authorized Optobionics Corporation to implant their Artificial Silicon Retina (ASR) in up to ten patients as part of a 2-year study. [OPTO00] Doctors have already implanted microscopic chips in the eyeballs of three patients suffering from retinal damage, in an attempt to determine whether the chips can restore human vision. [CNET01]. Several eye implant projects within the U.S. and Germany are implanting chips "on the surface of the retina, the structure at the back of the eye. Another eye implant project is putting its implants at the back of the retina, where the photoreceptors are normally found. These 'subretinal' chips may block the transport of oxygen and food to the overlaying nerve cells, so Eberhart Zrenner of the University of Tubingen, Germany is developing 'chain mail' electrode arrays, with plenty of holes for the delivery of supplies". [WELL99]

The doctors who are implanting microchips on the surface of the retina hope that the microchip will restore vision where blindness was caused by a hereditary condition known as retinitis pigmentos. The patients were implanted with an Artificial Silicon Retina chip that was created by the Illinois-based Optobionics Corporation.

22

[CNET01]. Because this is a first time ever procedure and the study is only in the very initial stages, no longstanding generalizations can be determined. So far, the company has noted from data gathered that "the implants continue to function electrically and remain stable in position and the patients are in no discomfort and living at home." [OPTO00] After the July 2001 surgeries of the ASR chip implants, although no reports of improved vision have been found, preliminary tests have determined that no complications have occurred; and the doctors plan to present the results at a future date to the public. [OPTO00].

The results of Eugene de Juan of John Hopkins Wilmer Eye Institute (Baltimore, MD) in Research and Development have also been noteworthy. His electrodes have been inserted directly in to the eye. He reports that completely "blind patients being able to see well-defined flashes, which change in position and brightness as de Juan changes the position of the electrode or the amount of current. In his most recent experiments, patients have identified simple shapes outlined by multiple electrodes." [WELL99].

The ASR chip was reported as smaller than the head of a pin and about half the thickness of a sheet of paper. The chip is powered by solar cells that convert light into electrical impulses, and also to help stimulate the remaining healthy retinal cells. [CNET01]. An ASR contains approximately 3,500 microscopic solar cells. The purpose of the chip is to replace damaged human photoreceptors, which is the light sensing cell of the eye; it normally converts light into electrical signals within the retina. [OPT00] Figure 5 is a close-up of a chip implant in the back of the eye.

Inner retina

Outer retina

Optic nerve

Lens

Iris

Cornea

Implant in the subretinal space
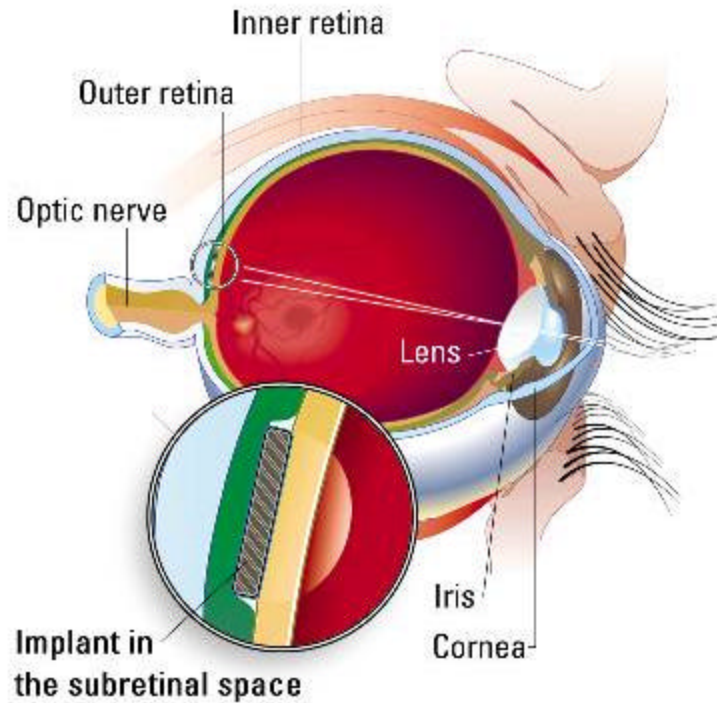
Drawing by Mike Zang

Figure 5.   Eyeball with Close-Up of Retina and Chip Implant in Area of Location
(taken from Optobionics Corporation Website: http://www.optobionics.com/).

b.   *Implantable Hearing Devices*

Recently the U.S. Food and Drug Administration (USFDA) has also approved the use of implantable hearing devices in limited instances of extreme hearing loss. As a result several companies have come into this business. The Nucleus Company has produced a product called Nucleus® 24 Contour. It is their premium product in a line of several Nucleus 24 implant family products. It is the first self-curling 22-channel electrode, which is giant step forward in electrode innovation. Their device "features included 22 channels for flexibility in hearing and programming, a titanium casing provides strength and reliability and uses Neural Response Telemetry (NRT), which measures the responsiveness of your cochlea (the spiral shape of the inner ear." [NUCL00]

c.   *Brain Implants*

Brain pacemakers (consist of an electrode permanently implanted in the brain) and are similar to heart pacemakers. Brain pacemakers use electrical stimulation

in the brain to maintain neural equilibrium. The electrode emits electric pulses from a power pack (about the size of a pager) in the chest. "Brain pacemakers were first successfully implanted in humans nearly 15 years ago in France, and in 1997 in the U.S. The FDA approved the first U.S. use of pacemakers to treat essential tremor and Parkinsonian tremor—currently, the only approved indications." [TECH01, p. 36] Doctors are able to implant an electrode into a small area of nerve cells within the thalamus, with the assistance of a hydraulic device. The hydraulic device advances the probe, containing the thin electrode, in micrometer increments. The desired affect is that when doctors "send an electrical current to the implanted electrode, the patients' tremor would diminish and perhaps disappear all together." [TECH01] Several weeks after her surgery and with doctors readjusting the settings on the pacemaker, Joan Sikkema has been overjoyed with the results. Her tests showed "80 to 90 percent improvement in her intentional tremor and 100 percent resolution in her postural tremor." [TECH01, p. 43] This form of surgery is only used in very extreme cases where all else attempted has failed and only on a few patients. It is only just now being considered for the treatment of other neurological conditions.

3. Human Microchip Implants

Heart and brain pacemakers have been in use for quite some time. However, the following section will discuss a new direction for implants in humans. The significance of most of the following implants is that they are not being used in life threatening cases or extreme life hindrances. These implants are being used as life enhancements, to offer convenience over traditional methods of living or just or something "nice to have" to provide a sense of self-security.

a. Soul Catcher 2025

Since 1996, there has been news and discussion about a research project under development in British Telecommunications (BT Labs). The reports reflect that BT Labs is working on a huge project to develop a memory chip that will be implanted behind a person's eye and will be able to record all the thoughts and experiences of that person's lifetime. [CSMA]

> This project is an outgrowth of BT Labs' artificial intelligence research, the project was given an initial $30 million in development funds. The Soul Catcher 2025 would attach directly to a person's optical nerve and

store incoming sensory impulses that could be downloaded and played on a computer or implanted in someone else's memory. 'A lifetime's worth of experience could be stored in about 10 terabytes,' according to Peter Cochrane, BT Lab's head of Advanced Applications and Technologies. [TEME01, p. 97]

However, in a conflicting report, the "team of eight Soul Catcher scientists, headed by Chris Winter, state that he says that he was misquoted by local journalists, intending to enthuse them about the future-looking work at BT Labs." [CSMA] Upon contacting BT Labs public relations department, Cynthia K. West, author of Techno-Human MESH, was sent an article along with a handwritten note from the information officer, stating that Soul Catcher is "very much a concept and not a product, or even an experiment." [TEME01, p. 97]

b.   *Sky Eyes*

British newspapers and periodicals reported that a company named Gen-Etics had patented a device for private use called Sky-Eyes. "Sky-Eyes are being used by Italian dignitaries who fear being kidnapped. They are having microprocessor homing devices planted in their bodies so police can track them down if they are abducted." [TELE98] "Sky-Eyes is reportedly made of synthetic and organic fiber and run on such a small amount of energy that this can be 'borrowed' from the human body." [TELE98] It is reported that a "person who carries this device is supplied with an eight-digit code by the company" and "advised not to reveal it to anyone except a next of kin or trusted legal representative." [TELE98] The reason that little is known about this company and its product may be due to their reports of use by an exclusive clientele, which include "film stars and children of millionaires", and the company's "concern to protect its clients." [MERC98], [TELE99]

c.   *Implants for Drug Delivery*

Between 1998 and 1999:

researchers at the Massachusetts Institute of Technology had created a prototype chip around the size of a 10-cent coin that contained tiny chemical reservoirs each sealed with a gold cap. At a preprogrammed time, a memory chip melts the cap by applying a small electrical voltage, releasing the chemical stored inside. [NSCI99]

Today, increasing numbers of medical devices are being manufactured as instruments that can be used inside the body to treat medical conditions. One such medical technology includes microscopic devices injected into the blood stream of a diabetic to monitor blood sugar levels and automatically trigger an insulin pump. This technology eliminates the need for daily insulin injections. [ISEPP]

Southern Biosystems (SBS) is a company that develops drug-loaded implants and also manufactures biodegradable polymers. Drug-delivery implants consist of an active and a polymeric excipient that are formed into a fiber, rod, film, or other. "An excipient is any part of a drug formulation that is not an active pharmaceutical agent. An example is an aspirin pill that contains binders and other ingredients to make the pill stay in pill form, but are not the active drug that cause any biological affect." [WATS01] They control drug release through a number of variables. Southern Biosystems typically works with biodegradable polymers to eliminate the need for removing the device. [SBS00]

Some people are willing to have medical devices implanted in their bodies or willing to use other medical technologies for convenience (microscopic injectable devices). The aforementioned observation may be an indication of the general population's willingness to use similar implantable devices for convenience, enhancements, and to better their standard of living. This willingness to enhance lifestyles may signal that, the gap that exists between human and machines is slowly closing.

d. Trans-Humanists

We are seeing a shift in thinking among our younger generation with post-secondary education. This generation may be viewed as being more flexible and open to highly philosophical issues that directly affect the very nature of our being and existence. One such philosophical area is that of "transhumanism". [NBOS00]

> 'Transhuman' is a shorthand term used to refer to a 'transitional human', a sentient being first described at length by the early generation futurist, F. M. Estfandiari as a potential step towards evolution into a posthuman. [TRHU99] A posthuman is a human descendant who has been augmented with artificial devices to such a degree as to be no longer a 'human'. Many transhumanists want to become posthuman. [TRHU99]   Calling

27

transhumans the 'earliest manifestation of new evolutionary beings,' F.M. Estfandiari suggests that some signs of transhumanity include bodily augmentation with implants, androgyny, asexual reproduction, and distributed identity. [TRHU99]

Many transhumanists already consider themselves transhuman, because our use of tools has greatly expanded the capabilities of the human body and mind. The trend is one of continuing progress in the development and use of global communications, body modification, and use of life extension techniques. Any human who takes advantage of this trend can achieve transhuman status within a lifetime. [TRHU99]

As far fetched as the topic of transhumanism may seem, there are several organizations that exist to promote interesting this issue, for example, the Swedish Transhumanist Association, the Aleph and Dutch Transhumanist Society, and World Transhumanist Association.

e. *Individual Human Microchip Implant Profile*

It has been reported that Prof Kevin Warwick, a professor of cybernetics at the University of Reading in the United Kingdom had a microchip implanted in the upper inside of his left arm in 1998. He describes that "his implant communicated via radio waves with a network of antennas throughout the department (of Cybernetics) that in turn transmitted the signals to a computer programmed to respond to his actions." [WIRE00]. Such connectivity allowed him to have his office door automatically opened for him as he approached and other similar simple tasks. The major objective of his experiment was to determine whether information could be transmitted to and from an implanted microchip. Professor Warwick was so pleased at his results that he has decided to perform a second, follow-on experiment with a new implant that would "send signals back and forth between his nervous system and a computer." [WIRE00] The results of Professor Warwick's second implant experiments will determine if his wife Irena will have a similar implant placed within her body as well.

Professor Warwick's first implant was placed on the "upper inside of his left arm, beneath the inner layer of skin and on top of the muscle." [WIRE00]. He plans for the next implant to be placed again in his left arm but in-between his elbow and shoulder, connected to the nerve fibers in that location. He purposely chose the left arm since he is right handed and hopes that if any problems arise he will suffer less manual

impairment. "Most of the nerves in this part of the body are connected to the hand, and send and receive the electronic impulses that control dexterity, feeling, even emotions." [WIRE00] He feels this is an optimal nerve center that is "large and quite strong" because it "carries more information than any other part of the anatomy, aside from the spine and the head", yet still has "very few nerve branch off points to muscles and other parts of the upper arm." [WIRE00]

In the second experiment a neurosurgeon, Ali Jamous, will surgically implant a transponder that will connect directly to the nerve fibers in Prof Warwick's arm. "The tiny glass capsule will have a power supply and three miniaturized circuit boards that will transmit and receive signals." [MSNBC] Prof Warwick's first task will be to send and digitally store the electronic signals that his brain sends to his hand when he wiggles his index finger. The ultimate desired effect is to have the computer's stored signal (of the initial instruction to wiggle finger) sent back to his brain and hand, via the microchip. The hope is for the finger to give the same wiggle response as before. [MSNBC] The second task will be experiments that "'record' Prof Warwick's neural signals when he is feeling happy, sad, angry, and scared." [MSNBC]

At this point, if the experiment continues to go well, then Prof Warwick's wife, Irena, will have a microchip implanted inside her; and they will both attempt to digitally connect via the Internet and try the wiggle finger experiment on one end to see if the other person's finger responds in a wiggle movement as well. This would represent a new way of "thought communication." [MSNBC]

Prof Warwick understands that his microchip implant experiments have large social implications, such as the 'Big Brother' issues of State control and surveillance; however, he feels that it "is important to raise awareness of what's already technically possible so that we can remain in the driver's seat" and "that as long as we're gaining things, we'll yell 'Let's have Big Brother now!' [MSNBC]

The next chapter will discuss conceptualizations, potential uses, visions, advantages and disadvantages of providing microchip and similar technology within the U.S. Navy.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. POTENTIAL USES FOR MICROCHIP IMPLANTS

The U.S. Navy uses various user identification devices to assist in properly identifying the user in order to check authorization for access to specific equipment or to specified areas. The UIDs recently in use are smart card and biometrics, which were briefly discussed earlier in Chapter I. Considering this and other recent advances in the intersection of life sciences with information technology, new concepts and visions will be explored in this chapter.

Speculation among academia, governmental, and private sectors continues to grow and futurists predict that microchips, computer devices, and other informational and computer technologies will be implanted into our bodies in the not too distant future. One such person quoted was Neil Gershenfeld, the MIT associate professor who assisted Thomas Zimmerman on his master's thesis.

> Neil Gershenfeld,…believes that in ten years we will be wearing computers and that twenty years from now, we will implant the computing devices into our bodies. Thirty years from now he thinks that we will use genetic engineering to grow the devices we desire. [TEME01, p. 26]

Of all of the radio frequency applications discussed thus far, the most intriguing and intensely debated is that of human microchip implants. Once again, this chapter will present the potential uses of microchip implants and defer the ethical implications for the next and final chapter. Because our technology is proving that the capabilities for human implants exist, discussion should begin with an examination of the purpose it could serve to the U.S. Navy. The following section will outline, some possible benefits and detriments of human microchip implants.

A. CONCEPTUALIZATIONS FOR MICROCHIP IMPLANTS

Today many people not directly involved in the science and technology fields are beginning to realize that human microchip implants are physically possible. For example, find below a quote from a well-read periodical, *PC Computing*:

> How'd you like to avoid waiting in lines for the rest of your life? Breeze through everywhere like you owned the place. Watch lights snap on, doors open automatically, money pop out of ATMs as you approach. Never have to show an ID, buy a ticket, carry keys, remember a password. You'd

leave stores loaded with packages and waltz right past the cashiers. You wouldn't have to carry a wallet. Ever. Family and friends could find you instantly in any crowd**. There's only one catch—you'd need to have a tiny little chip implanted in your body. No big deal.** (Paul Somerson, "Inside Job", PC Computing, Oct. 1999, p. 87)

American government, particularly those entities involved in space and computer sciences, is taking a step toward looking at all the technological capabilities available. Naval Space Command is one such entity. "Naval Space Command (NSC) is the SATCOM System Expert under U.S. Space Command (USSPACECOM) for the Global Broadcast Service (GBS). An element of GBS that is being wrestled is Information Dissemination Management (IDM)." [TRAM00] There are many topics for discussion under IDM. One of the topics, user identity, had been submitted to the NPS Space Chair as a potential thesis topic by Mr. Emmett Henderson, one of the subject matter experts in GBS at Naval Space Command. User identity is being explored in a continuing effort to positively identify and ensure the right person is receiving information that is being disseminated. Mr. Henderson has been very involved in IDM concerns and is one of few who believe we should consider embedded identity schemes such as human microchip implants. Mr. Henderson suggests that human microchip implants should be considered and studied as a means of one day achieving that positive electronic identification for humans. [HEND00]

> Scientists have been able to grow nerve cells of a rat on a silicon chip— and have transmitted electrical impulses through the cells to the chip. Eventually, it should be possible to take human brain cells and connect them directly to a computer. Silicon chips, for instance, could be implanted in the brain, thus combining different kinds of intelligence, the best of quantitative and qualitative intelligence. [WHIT99]

The following sections lists the potential uses for passive and active microchip implants and some of the risks that can occur for both.

B. ADVANTAGES AND DISADVANTAGES OF HUMAN MICROCHIP IMPLANTS

1. Potential Uses (Advantages) for Passive Microchip Implants

There are a wide range of advantages to the use of passive microchip implants in humans.

- Microchip implants could identify the military member, as the military ID card does now. Even more data could be held within the microchip.

- Unlike the current physical military ID card, a military member would be unable to lose or misplace their implanted microchip, (barring its possible migration within the body). The likelihood of UID being stolen from the member would be decreased.

- The implanted microchip could facilitate routine events with limited intervention, and would reduce clerical error. For example, the check in process for military members at medical facilities could be made more efficient. There would be less wait time in lines at the main check-in area or later substations.

- Electronic transactions could easily occur by just scanning the microchip implant area. The check-out process at supporting facilities (e.g., NEX and commissary) could be expedited.

- The implanted microchip could replace the need to carry business financial cards and any e-transaction cards (credit, debit, smart card). There would be no need to issue government credit cards to individuals.

- The implanted microchip could replace the need to handle cash.

- The implanted microchip could replace driver's license and social security cards, and health records. This type of replacement or improvement may reduce the possible misplacement of paperwork. It could also eliminate large amounts of physical space needed to maintain documents as we currently do. Military members would not have to physically carry original documents from duty station to duty station or from medical facility to civilian facilities if needed. The microchip implants could also offer a continuous record of medial history reducing human error.

- The implanted microchip could replace "memorized" passwords and personal identification number (PIN) usage in all electronic aspects and in all environments.

- With a strong backing between the microchip and its carrier, many new uses are possible. [HEND00]:

  - The microchip could easily grant access to secure facilities.

  - The microchip could easily grant individuals access to various computer terminals and a predetermined range of sensitivity level access to them. For example, an individual with a verified microchip could be granted access to a secret area and once inside be further granted access to a top secret area housed within the first level secret area.

  - The microchip could be used in conjunction with smart weaponry. For example weapons could be designed with a microchip and

would be programmed to not fire unless a properly authorized user is identified.

- Secured areas and valuable assets would remain locked until an authorized person with microchip matches preset access information. This could eliminate the need for human security guards.

- Perhaps telephones could passively read your positive microchip ID and transmit it to those with whom you are talking, instead of simply sending your telephone number. [HEND00] This could possible be an advanced method of caller ID.

- The implanted microchip could be used as a national universal identity device and every human could have one.

2. Potential Uses (Advantages) for Active Microchip Implants

The advantages of active microchip implants are listed here.

- The implanted microchip could be used to locate missing military personnel. Military members who may be AWOL, POW, Leave, or on Liberty.

- The implanted microchip could be used to help locate and track children, teenagers, elderly, and loved ones. For example if a personal is involved in an accident but their body can not be seen, the active microchip would be able to assist in locating the individual who might be in life threatening danger.

- The implanted microchip could hold digitally encoded biometric data. Once the implanted microchip has been scanned for information, the output could be a projected image of "user" and vital statistics for identification purposes. This information could possibly be displayed onto a "smart board", eye visor or some visual interface hardware. Possible vocal effects of individual with the microchip implant could also enhance the identifying biometric characteristics.

- Potential microchip implants into military members could possibly provide "real-time" statistics of human resources at a particular location (or battlefield). This data could be relayed back to requesting command. Use of a pre-determined universal language understood by all military members could be required to stimulate accurate decision making.

- Microchip implants could be used in the transfer of information from one human to another (or group). For example the aforementioned scenario could mimic the current capabilities of hand-held personal digital assistants (PDAs) when transferring information to each other.

3. Potential Risks (Disadvantages) of Either Type of Microchip Implants

There are many potential problems with microchip implants. This section lists several.

- Physical harm and malicious activities could be brought upon humans who have microchip implants. Potential identity theft could be the desired result of this offensive behavior.

- The capability of updating and servicing the microchip implants is risky and at this point questionable. If the need arises to correct the operational function of the microchip, the efforts of reimplanting a repaired microchip may not be worth the effort of servicing it. The less invasive method of administering the new microchip is preferred. It is doubtful that easy re-administration of a microchip can be accomplished considering how fast our technology changes.

- Database management is a top concern when microchip implantation is considered. Questions regarding who would control the data held in the database system need to be considered. For example, which entity is sufficiently trusted to be responsible for managing it? How does one control and prevent the unauthorized access to this data (database subversion)?

- Public fears of implementing a human microchip implantation program would arise if prior consideration of second and third order effects are not taken into account. This would raise doubt as to the effectiveness and integrity of data held on the chip.

- Microchip implants could cause fears of personal privacy being severely deteriorated, or worse, ceasing to exist. This is of particular concern when people feel they are under round-the-clock surveillance, especially within the confines of their homes.

- Undetermined or inconclusive evidence of health effects of radio frequency emissions is a concern. [CIR01]

- People may have fears and doubts as to the integrity of the microchip implant data from manufacturer. There would be concerns of tampering at the manufacturing level. Manufacturer security procedures and policies would require highly rigorous configuration management and regulation.

- Individuals would also have concerns of the overall integrity of the data at the issuing entity's location. An example would be someone's desire of a guarantee that the wrong identification device is not being implanted inside them. Since individuals cannot easily see or touch the identifying number, their new usage would be minimal, if it exists at all. Also the individuals might question the use of unauthorized readers, or reader devices.

- Although active chips can offer read-write capabilities, unlike passwords, once an ID number is created for a chip, it cannot be easily changed at the users' secret desire.

As any progress in the area of human microchip implants is being researched, serious consideration and thought need to be directed toward the equally great concern of various philosophical and intangible issues. These concerns will be addressed in the next chapter.

V. SOCIAL CONSIDERATIONS OF UIDS

Numerous issues beyond the detailed technical and sheer operational capabilities of microchip implants must be considered. Prior to suggesting the use of microchip implants, extensive time and resources will be required to examine all facets of their use. If the infrastructure and the processes are set into motion without an in-depth investigation of all issues, then many questions will go unanswered. Due to the large number of considerations that must be undertaken, only a few intangible and theoretical considerations such as security, privacy, social, ethical, and future considerations will be presented here.

A. SECURITY AND PRIVACY CONSIDERATIONS

Security and privacy are key concerns in the management of automated computerized systems and processes. Although at times difficult, security and privacy issues must be carefully managed. This section will focus on the security vulnerabilities that challenge wireless systems (and similar systems that use RFID technology), such as confidentiality, data integrity and data authentication.

1. Security of Communications

a. Confidentiality

In the communications environment maintaining confidentiality is important. Confidentiality can be defined as being "of classified or sensitive data, the degree to which the data have not be compromised; assurance that information is not disclosed to unauthorized persons, processes, or devices" [ITS00] When using radio frequency technology and microchip implant technologies one must be certain that the information transmitted from a valid source is only received by the intended recipient, without a breach.

(1) Potential Threat. There can be several threats to confidentiality. The most common is that of eavesdropping. Eavesdropping is easily achieved in the radio emissions environment. When communications take place over the radio waves, everyone who is equipped with a suitable transceiver within the range of transmission can eavesdrop on that occurrence. The intended receiver is unaware of the eavesdropping because the receiver has no physical means to know that other reception

has taken place. [SAMI97]. The frequency band and transceiver power used has a great effect on the range where the transmission can be heard. Depending upon the frequency used and the transceiver power, the communications of a wireless system can be eavesdropped from outside the building in which the network is operating. This will occur provided there is no special electromagnetic shielding. The emissions that do not stay bound to the interior of protected structures will be susceptible to unauthorized exposure. [SAMI97]

The impact of eavesdropping can depend upon the value of the information that was compromised. When eavesdropping has occurred, unauthorized individuals may gain valuable information. These individuals can continue to gain more information for their benefit and cause anywhere from financial to life threatening disasters or even loss of life.

(2) Potential Countermeasure. In the wireless environment eavesdropping is difficult to deter. The two privacy defenses to eavesdropping are encryption and shielding. Encryption involves scrambling the transmission so that only those with the appropriate key can decrypt it easily. [SCHN96] Shielding the transmission of electromagnetic energy signals is also a good defense. However, providing good shielding will have an affect upon the signal transmission range.

b. Data Integrity

Data integrity refers to keeping data free from unauthorized modification or corruption (subversion). [CS3600] Decisions can be made upon corrupted, inaccurate data, causing a chain reaction until these inaccuracies are found. Depending upon the time frame that the corrupted data is found, it could be too late to correct. For example if the inaccuracy caused unauthorized persons to gain access to an area outside of his or her scope of responsibility then he or she could destroy information or assets or gain privileged information.

(1) Potential Threat. An example of a potential threat to data integrity would be a modification of stored data on the microchip. If at the manufacturing plant, the microchips are placed on storage shelves without security personnel then someone could tamper with the microchip ID number. Another example would be modification during transmission when a microchip is being scanned or read. If

someone is getting their microchip implant data scanned into a system and an "outsider" has access to this transmission, as explained in eavesdropping, they could potentially modify it and re-transmit incorrect information.

        (2)   Potential Countermeasure. Certainly, universal standards, policies and procedures can help to ensure that the data residing on the microchip is accurate, and difficult to modify in each and every step of the process from the manufacturing plant to the final issuing entity. An example of such procedures is a system of "checks and balances" where neutral parties assist in assuring correct steps are taken throughout each phase. Cryptographic "sealing" or signing, can also provide protection of stored or transmitted data from unauthorized modification.

c.   *Authentication*

Authentication in the context of identification "is the establishment of the validity of a claimed identity." [TCSEC] The difficulties of identifying the "claimed identity" can be increased with any user identification device due to the inability to unequivocally validate the actual person linked to the identification tool. It is therefore crucial to institute reliable authentication mechanisms for the security of an identification system.

        (1)   Potential Threat. The main threat with regards to authentication is personal identity theft. A person who has stolen the user identification device of another and uses it to impersonate him or her, serves as a common example. Since user identification devices in effect identifies the innate object itself and not the human, additional means of establishing identity is required.

        (2)   Potential Countermeasure. There are three ways to authenticate a user of a system or area; by means of "something one knows", "something one has", and "something one is". The most popular process of authenticating an individual user to a system is through the use of a password. For example, when one requires entry into a computer they enter username and then a "password" that only he or she has knowledge of. This password is the authenticating measure to augment the individual's access. In the case of "something one has", the authenticating measure usually is a physical device such as badge or a key. For "something one is", biometrics are used such as such as an iris pattern, or a fingerprint.

2. Privacy of Information

As a whole, humans closely value a sense of freedom and privacy. While there are variations to its formal definition, privacy can be defined as "freedom from the intrusion of others in one's private (personal) life or affairs…" [RAND99] Many however, view privacy as a "right, legal, and absolute standard" that is one of our inherent civil liberties. [CLAR97]

"Information privacy," as defined by Roger Clark, is the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves. [CLAR97] Legislation has been passed to protect the information privacy of individuals. One such act is the Privacy Act, Public Law 93-579 (1974), which requires U.S. government to safeguard personal data processed by federal agency computer systems and provide ways for individuals to find out what information is being recorded on them and a means to correct inaccuracies. In many countries, the concept of privacy has been fused with data protection, which interprets privacy in terms of management of personal information. [GILC]

It is because of technical advancements that it is difficult for both of these elements, security and privacy, to completely coexist in certain environments. One may tend to over-shadow the other. As society enters the information age era, where technology is out-pacing other issues, it has caused humans to seriously make privacy rights a high priority and form alliances for the protection of privacy throughout the world. [GILC] The next section will present the human response to the information age.

B. ETHICAL CONSIDERATIONS

In her book, *Techno-Human Mesh: The Growing Power of Information Technologies*, author Cynthia West explains that in order to understand the interface of the humans and machines, now and in the future, we must have a basic understanding of some theoretical issues. To understand the effects that technical advancements are placing on human kind, we should gain a basic comprehension of the theoretical underpinnings of the human "body," the political and environmental status of the "body" and the intersection of knowledge and power upon the "body." [WEST01, p. 153] It is from various feminist theories of the physical human body, the dualistic theories of the human body and it's devaluation associated with females, slaves, and the disenfranchised

that places the human body in a highly political position-"a site of power." [WEST01, p. 158]   West also believes this conceptual understanding sets the stage for the permissibility of human bodies of any gender, race, class, or sexual orientation to be attached to the disciplinary power networks of information technology. "This devalued conceptual status of the physical body is the foundation that contributes to the current and future status of body-human machine integration in information technology." [WEST01, p. 158] In other words, Cynthia West purposes that our history proves that the value we have placed upon the human body based upon historical views of women, slaves and other economically challenged groups placed the human body in the political power struggle spotlight. It is from this basis that permissive or non-permissive consent of humans are attached to the disciplinarian power options of information technology.

Speculation continues to grow as to which groups of the human population will have microchips introduced into their bodies to test the feasibility of the concept and for further future implementation. Some have eluded to the fact that eventual human microchip implantation is coming and is possible. These people believe that it will first be on a volunteer basis [RAMI97] and then the government will intervene making it mandatory in the penal system and military.

1.   Mandatory Human Subject Programs

A few examples below are of systems/programs targeting human subjects that were implemented without the consent of the individual(s) it was performed upon. These examples stirred a highly ethical debate among many people and a few lessons learned can be gathered from these mandatory programs.

a.   Anthrax Program

In 1998, after a series of tests and studies DOD began mandatory vaccinations against the biological germ weapon called Anthrax. Anthrax is produced by the bacteria *Bacillus anthracis* and is highly lethal. In May 1998, then Secretary of Defense, William Cohen approved the vaccination program to ensure that by 2005 all military members between ages of 18 and 65 and emergency essential DOD employees and contractors assigned to high threat areas are vaccinated against this biological weapon. Although there has been documented resistance by about 16 military members, the program still exists. There has been a recent temporary "slow down," which DOD

has stated is due to a limited supply of FDA released vaccine. [ANTH00, OASD98] As DOD has dealt with the public relations problems caused by these members' initial refusal to be vaccinated due to health concerns, debate continues regarding social and ethical issues that must be considered. [BATE01]

b. *General Vaccination Programs*

There are several vaccination programs within the United States to protect individuals from succumbing to diseases. Although they vary by state as to the schedule, the majority of the vaccinations occur to school age children. General vaccinations occur for adults in preparation to travel to different countries and for the military various mandatory programs such as the flu shot program and the Anthrax program mentioned above. Few U.S. citizens have questioned the safety and effectiveness of the general vaccination programs. For example, according to Hugh Fudenberg, MD, a leading immunogeneticist, if an individual has had five consecutive flu shots between 1970 and 1980 (the years studied) his/her chances of getting Alzheimer's Disease is ten times higher than if they had one, two or no shots. [TEDK01] In 1976, President Ford made a decision for a national inoculation against the swine flu, which is still debated today. [FLU]

c. *Military Draft Registration Program*

President Franklin Roosevelt signed the Selective Training and Service Act of 1940 which created the country's first peacetime draft and formally established the Selective Service System as an independent Federal agency. [SSS01] From 1948 until 1973, American men only were drafted to fill vacancies in the armed forces. In 1973, the draft ended and the U.S. converted to an All-Volunteer military. After a 5-year suspension, President Carter resumed the registration requirement in 1980 in response to the Soviet invasion of Afghanistan. "Registration continues today as a hedge against underestimating the number of servicemen needed in a future crisis. The obligation of a man to register is imposed by the Military Selective Service Act. The Act establishes and governs the operations of the Selective Service System. [SSS01]

2. Ethical Issues of Mandatory Programs

One definition of ethics as defined by Industry Canada-Life Science Branch is that "Ethics is the activity of thinking about and deciding how people ought to act in their relationships with one another, and about how human institutions and activities ought to

be organized." [ICLS01] In another definition it is "a philosophical system, or code of morals that serves as a standard of conduct and moral judgment." [TEME01]

The Markkula Center for Applied Ethics states that ethics should not be entirely defined by and individuals' "feelings, or by following the law, or social norms or be identified with religion, all of which can deviate from what is ethical." [MCAE] The Center's supporting examples are; "a person following his or her feelings may recoil from doing what is right." Although religion promotes ethical behavior, such behavior cannot be confined to religion, nor is it entirely equitable to religion. Finally, pre-Civil War slavery laws in the United States and apartheid laws in South Africa, are examples of how laws can deviate from ethical behavior. [MCAE] However, people have a need to rationalize and reason in order to balance the decisions and choices they make about themselves.

Among the factors that most influence ethical behavior are personal behavioral lessons learned as a child; these are among the most important. People consolidate these lessons into individual morals, self-imposed standards and values. These morals, standards and values become the foundation of how an individual "feels" or "perceive" himself or herself. These morals, standards and values also help determine how the individual interacts with other members of people in society. When people go about their daily lives, and are faced with events and situations that go against their ethical foundations internal conflict can result. No longer are people merely functioning in a realm of purely right and wrong. "Ethical analysis and decision making occur at various levels, ranging from the individual to the societal and even the international. Sometimes, conflict may emerge among choices made at these various levels." [ICLS01] We strive to gain knowledge and create items to make our lifestyles more safe and convenient. Today we realize a struggle between advancing our species with information and science technology for great benefits but at the same time these advancements contradict many individuals' ethical beliefs or feelings.

Mandatory programs are coming under greater public scrutiny. Perhaps one can study historical mandates to predict a partial interpretation of the reception that will be shown if human implants for identification purposes were to be made mandatory in the

military. In his article, "Mandatory Vaccination Programs and Medical Ethics," Dr. Miguel A. Faria, Jr., discusses how issues of mandatory vaccination programs for infants and children has become tense among concerned parents and physicians. [MAFJ01] Dissenting physicians are teaming with concerned parents, both groups troubled by the side effects of vaccines. These side effects can include serious neurological deficits and in some cases can cause death of the infant or child. "The physicians on this side of the debate are calling for more open data and information to the public; have questioned oft-cited risk versus benefit figures; and call for a return to the individual-based ethics of Hippocrates: particularly, first do no harm." [MAFJ01] On the other side of this debate are government officials, and other organized health community representatives. Of course these representatives are at the other end of the spectrum, where they want the government to take a more active role in developing a technologically advanced vaccination program.

"The Tucson, Arizona-based Association of American Physicians and Surgeons (AAPS) is a group that is supports increased parental involvement and freedom of choice in the vaccination decision." [MAFJ01] With full disclosure by the responsible governing body, the AAPS believes that parents should have the right to decide whether or not they will subject their children to certain vaccines. But this certainly wouldn't carry over for the military member. When mandatory programs are instituted in the U.S. military, non-compliance is met with serious consequences. Unlike the civilian sector the military operates under different standards and regulations. For example, with the implementation of the mandatory Anthrax program, there have been several instances where court-martial has been determined and restrictions and reductions among military members has occurred.

In 1998, 16 military members (14 Navy and 2 Air Force), whiled stationed in the Gulf refused to take the anthrax inoculations. As a result, two sailors were discharged from the Navy for "disobeying a lawful general order." The others were given 30 days restriction to the ship, 30 days extra duty, reduction in pay for one month and/or reduction in rank. The reason given for the two sailors' dismissal was the inclusion of previous discipline problems where they had "demonstrated a pattern of misconduct." This refusal also came about at the time the military had just begun to inoculate

approximately "37,000 U.S. military members." There had already been "15,000 Navy personnel" who received the inoculation, and all the military members who had received the shot were stationed in the gulf at the time. [CNN98]

After reviewing a few mandatory programs, and analyzing today's human adaptation to technology advancements, a sequence of reactions that one may possibly expect if the U.S. military were ever to implement a mandatory microchip implant program would be (in order): [HEND00]

- Non-belief
- Belief
- Fear and loathing
- Fear
- Being uncomfortable
- Understanding
- Comfortableness
- Acceptance
- Demand (the high point of acceptance)

Perhaps demand may continue to increase; "the populace will demand the services because they cannot maintain the quality of life they desire without them." [HEND00]   If human microchip implants are ever to be implemented then all the ramifications must be studied and well thought through by all entities.

THIS PAGE INTENTIONALLY LEFT BLANK

VI.   CONCLUSIONS AND FUTURE CONSIDERATIONS

User identification devices are important tools in the military as well as the civilian sector. The need to ensure the right person gains access to the appropriate information, equipment, and/or area is paramount in the daily operations of defense.

Accurate identification cannot be compromised. Very low tolerance for errors in identifying individuals is acceptable. Unfortunately, in today's society, misidentifications still occur and as a result can cause irrevocable and sometimes fatal events. To ensure communications and access is given to the correct or intended person, institutions are continuing to make improvement to the tools they use in the identification process.

A.   CONCLUSIONS

The objective of this thesis research was to explore the latest technologies available that offer improvements to the user identification environment. Research in the area of radio frequency identification technology was performed to understand its basis for noncontact identification. Once various applications of radio frequency identification were studied, devices currently being used and considered for use, were found mostly in the medical field. Industry is utilizing smaller devices that are carried on the person to assist them in identification. The private sector has made large progress in utilizing the latest identification technology available.

It is becoming highly likely that the government and private sectors will look for more absolute ways of identification. Human microchip implants can offer an improved means of identifying personnel and to give them access to controlled areas and assets. But what price is paid for this superior technology? Human microchip implants are currently not implemented in the U.S. military nor are they being considered to my knowledge. Although this paper introduces many possibilities, the author suggests that time be taken to perform a careful analysis of these possibilities and their secondary and tertiary effects before a time comes when they are considered or implemented. A delicate but strong balance, between technology and human usage of it, must be reached to ensure that the essence of our existence is not overshadowed by our desires to use technology

and be innovative. There can be enormous consequences to the technology human microchip implantation offers, but the possibility of the gaining benefits from its use and the technology advancements it could produce, maybe are equally as great as the risk.

B.   FUTURE CONSIDERATIONS

The author does recommend future military studies into the area of microchip implants for inanimate objects and humans. This subject is sufficiently complex to involve two master's students particularly one from the engineering field and one from the computer technology fields. A thorough technical study needs to be performed, especially within the area of security. These technical and security studies may help to gain the populace faith in the event a proposed human microchip implant program is pursued. To assist the human populace in gaining the confidence factor, the mechanical function and performance of this identification device program should be assured next. Also, in-depth psychological and social impacts upon individuals and community (to include political as well as ethical issues) and their long term impacts must be considered. Once these studies have been thoroughly performed and if the decision to continue has reached consensus, then the fiscal and operational constraints may be explored. Due to the ethical boundaries and codes we as humans live, an internal balance and rational maybe greatly needed to continue efforts in this type of identification schema.

LIST OF REFERENCES

[ADS00]   Applied Digital Solutions, [www.digitalangel.net/ceo/index.htm]. Nov 2000.

[ADS01]   Applied Digital Solutions, "Applied Solutions Forms Strategic Alliance With AT&T Wireless For Its Digital Angel Delivery System." [www.digitalangel.net/press/pr_2001/pr_2_7_01.htm]. February 7, 2001.

[AIM00]   AIM Global, [www.aimglobal.org]. 2000.

[AMEX]   Telephone conversation between American Express Blue Customer Service, and author, 27 June 01. and [http://www25.americanexpress.com/cards/Fmacfservlet?38/2351/b/3/0/247164603529/0/n&from=41].

[ANTH00]   Office of Secretary of Defense, "Anthrax Vaccination Immunization Program (AVIP)" [http://www.anthrax.osd.mil/Flash_interface/default.html].

[ARKI01]   Telephone conversation between Mr. Steve Arkinson, Project Engineer, Applied Digital Solutions, 14 Mar 2001.

[AVID]   AVID "Canadian Standard" Microchip, [http://www.avidcanada.com/avid/ac_chip.htm].

[BATE01]   Bates, Maj Sonnie, [http://www.majorbates.com/].

[BIOG]   Biometric Group, Inc., [http://www.biometricgroup.com], [iris-scan.com], September 2000.

[BMO01]   Biometric Management Office, [http://www.c3i.osd.mil/biometrics/] and [http://www.c3i.osd.mil/biometrics/index2.htm]. 2001.

[BOWE94]   Bower, Leslie A., *Automatic Identification Technology (AIT): The development of Functional Capability and Card Application Matrics,* Master's Thesis, Naval Postgraduate School, Monterey California, September 1994.

[CHOM01]   Interview and observation with duty staff nurse in maternity ward unit, Community Hospital of the Monterey Peninsula (CHOMP), Monterey California, 18 August 2001.

[CIRF01]   "Consumer Information About Radio Frequency Emissions", pamphlet distributed by Verizon wireless to their cell phone customers.

[CLAR97]   Clark, Roger,
[http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html#Intro].

[CNET01]   CNET News.com, "Chips implanted to restore vision."
[http://news.cnet.com/news/0-1006-200-6743452.html]., August 2001.

[CNN98]   CNN, "16 Gulf Troops Refuse To Take Anthrax Shots."
[http://www.cnn.com/US/9804/08/vaccine.revolt/]. April 1998.

[COCH]   Cochrane, Peter, [http://www.projectfreedom.cng1.com/the_beast.html].

[CSMA]   Howard, Toby, "Ghosts, Computers, and Chinese Whispers,"
[http://www.cs.man.ac.uk/aig/staff/toby/writing/PCW/upload.htm].

[DEST]   Destron-Fearing, "Summary of Field Studies Evaluating the Efficacy of
BioBond," [www.destron-fearing.com/elect/report.html].

[ELEC01]   Electronics ID Inc., "Implantable Transponder TX1400L."
[www.electronicidinc.com/tx1400l.html]. Jan 2001.

[FINK99]   Finkenzeller, Klaus, *RFID Handbook, Radio-Frequency Identification
Fundamentals and Applications*, John Wiley & Son, LTD, 1999.

[FLU] Mickle, Paul, "1976: Fear of a great plague."
[http://www.capitalcentury.com/1976.html].

[GARF00]   Garfinkel, Simson, *Database Nation*, O'Reilly, 2000.

[GILC]Global Internet Liberty Campaign (GILC), "Members."
[http://www.gilc.org/about/members.html].

[GSAA00]   "GSA Awards Government-wide Smart Card Solutions Contracts to 5
Prime Companies Contracts Worth Maximum of $1.5 Billion Over 10 Years",
[http://www.gsa.gov/Portal/browse/channel.jsp?channelId=-
12923&channelPage=/channel/default.jsp&cid=1]. then see GSA News release #9686,
May 2000.

[HEND00]   Email correspondence between Mr. Emmett Henderson, SME Global
Broadcast Systems, Naval Space Command, and the author, 25 August 2000 and 29
August 2000.

[ICLS01]   Industry Canada-Life Science Branch, *"Whose Values? Who Decides?"*,
[http://strategis.ic.gc.ca/SSG/bb00013e.html]. July 2001.

[IEEE00]   IEEE, "IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)." [http://grouper.ieee.org/groups/802/15/pub/WPAN-FAQ.htm] 2000.

[IETG4]   IEEE, "802.15 WPAN™ Task Group 4 (TG4)", [http://www.ieee802.org/15/pub/TG4.html].

[IMT00]   "Individual Microchip Technology", [http://www.networkusa.org/fingerprint/page5a/fp-chip-faq.html]. Jan 2000.

[IPEC]   IPEC-Americas, Inc., [http://216.117.129.17/public/faqs.html].

[ISEPP]   Institute for Science, Engineering and Public Policy, [http://www.isepp.org/Pages/01-02%20Pages/BioSci.html].

[ITS00]   Institute for Telecommunication Sciences, "Confidentiality," [http://www.its.bldrdoc.gov/projects/t1glossary2000/_confidentiality.html]. August 2000.

[IVES01]   Email correspondence Dr. Robert Ives, Professor of Electrical Communications at NPS and the author, September 2001.

[KOCH01]   Kocher, Dr. Frank, Veterinarian, Interview between Dr. Frank Kocher, Veterinarian, and author Oceanview Veterinary Hospital, Pacific Grove, 09 March 01.

[KURZ99]   Kurzweil, Ray, *The Age Of Spiritual Machines: When Computers Exceed Human Intelligence*, Viking, 1999.

[MBMS]   Kossel, M., Bendickter, Peter and Bachtold, "Microwave Backscatter Modulation System, [http://www.ifh.ee.ethz.ch/~kossel/TH2A-6.pdf].

[MCAE]   Markkula Center for Applied Ethics, "What is Ethics?"

[http://www.scu.edu/SCU/Centers/Ethics/practicing/decision/whatisethics.shtml,

writings], from 1995-1998.

[MERC99]   Dougherty, Jon E., "Concern Over Microchip Implants" [http://www.mercola.com/1999/oct/3/concern_over_microchip_implants.htm].

[MSNBC]   Masterson, Ursula O., "A Day with 'Professor Cyborg,'" 'http://www.msnbc.com/news/394441.asp?cp1=1].

[MURR01]   Murray, Bill, "'Long Way To Go' on Smart Cards," *Federal Computer Week*, p. 14. 11 June 2001.

[NBOS00] Bostrom, Ph.D., Nick, [http://www.nickbostrom.com/cv.html].

[NSCI99]   News in Science, [http://www.abc.net.au/science/news/stories/s18502.htm]. January 1999.

[NUCL00]   Nucleus Products, [http://www.cochlear.com/rcs/cochlear/publisher/web/products/implants_p/index.jsp].

[OASD98]   Mr. Kenneth H. Bacon, ASD (PA), DoD News Briefing. [http://www.fas.org/news/usa/1998/04/t04141998_t0414asd.html]. April 1998.

[OPTO00]   Optobionics Corporation, "Clinical Trials." [http://www.optobionics.com/clinicaltrials.htm, http://www.optobionics.com/00063pressrelease.htm].

[RAMI97]   Ramesh, Elaine M., "Time Enough? Consequences of Human Microchip Implantation." [http://www.fplc.edu/risk/vol8/fall/ramesh.htm].

[RFID96]   InfoPet Identification Systems, [http://rfidnews.com/la_rel.html]. 1996.

[SAMI97]   Sami Uskela, [http://www.tml.hut.fi/Opinnot/Tik-110.501/1997/wireless_lan.html#pahlavan97].

[SBS00]   Southern BioSystems, [http://www.southernbiosystems.com/drug-loaded_implants.htm].

[SCHN96]   Schneier, Bruce, *Applied Cryptography,* John Wiley & Sons, 1996.

[SSS01]   Selective Service System, "Background of Selective Service." [http://www.sss.gov/backgr.htm]. June 2001.

[TCSEC]   "Department of Defense Standard, Department of Defense Trusted Computer System Evaluation Criteria." [http://www.dynamoo.com/orange/fulltext.htm]. December 2001.

[TECH01]   Hall, Stephen S., "Brain Pacemakers." *MIT Technology Review*, pp. 34-43, September 2001.

[TEDK01]   Koren, Dr. Ted, "Vaccine Tidbits", [http://www.atlaschiro.com/ted_koren.htm#The%20Hepatitis%20B%20Vaccine]. September 2001.

[TELE98]   Johnston, Bruce, "Microchip Implants to Foil VIP Kidnaps" [http://www.telegraph.co.uk.]

[TEME01]   West, Cynthia K., *Techno-Human MESH, The Growing Power of Information Technologies*, Quorum Books, 2001.

[TIRF00]   Texas Instruments, "Texas Instruments Radio Frequency Identification Systems (TIRFID)." [http://www.ti.com/tiris/main.htm] 2000 and "Security Access and Convenience for Express Parcel Couriers."[http://www.ti.com/tiris/docs/solutions/solutions.shtml]. 2000.

[TRAM00]   Email correspondence between Mr. John Trammell, Naval Space Command, and the author, 25 August 2000.

[TRHU99]   The Transhumanist FAQ, [http://www.transhumanist.org/].

[TUTT97]   Tuttle, John R., "Traditional and Emerging Technologies and applications in the Radio Frequency Identification (RFID) Industry." IEEE Xplore Database, pp. 5-8, 1997.

[UKNEWS]   "Flaw found in common encryption program." [http://uk.news.yahoo.com/010803/12/c0d91.html]. August 2001.

[WATS01]   Watson, Scott, Director, Commercial Operations of Birmingham Polymers, Inc., Email Correspondence to author, received 18 September 2001.

[WELL99]   Wells, William, "The Chips are Coming." [http://www.accessexcellence.org/AB/IWT/biochip.html]. 1999.

[WHIT99]   Whitaker, Reg, *The End of Privacy*, The New Press, 1999.

[WIRE00]   Warwick, Kevin, "Cyborg 1.0." [http://www.wired.com/wired/archive/8.02/warwick.html,]. February 2000.

[WSJ01]   Warren, Susan, "'Ready-to-Wear' Watchdogs", *The Wall Street Journal*, Section B1, 10 August 2001,

[ZIMM95]   Zimmerman, Thomas, *Personal Area Networks (PAN): Near-Field Intra-Body Communications*, Master's Thesis, Massachusetts Institute of Technology, September 1995.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
    Ft. Belvoir, VA

2. Dudley Knox Library
    Naval Postgraduate School
    Monterey, CA

3. Carl Siel, Space and Naval Warfare Systems Command
    PMW 161
    San Diego, California

    ───────────────

4. Ms. Deborah M. Cooper
    Deborah M. Cooper Company
    Arlington, Virginia

    ───────────────

5. Ms. Louise Davidson, N643
    Arlington, Virginia

    ───────────────

6. Mr. William Dawson
    Community CIO Office
    Washington DC

    ───────────────

7. Ms. Deborah Phillips, Community Management Staff
    Community CIO Office
    Washington DC

    ───────────────

8. Capt. James Newman, N64
    Arlington, Virginia

    ───────────────

9. Major Dan Morris, HQMC, C4IA Branch
    Washington, DC

    ───────────────

10. Mr. Richard Hale, Defense Information Systems Agency
    Falls Church, Virginia

    ───────────────

11.	Ms. Barbara Flemming, Defense Information Systems Agency
	Falls Church, Virginia

	_____

12.	Mr. Michael Green, Director, Public Key Infrastructure Program Management
	Office
	National Security Agency
	Ft. Meade, Maryland

	_____

13.	Dr. Cynthia E. Irvine, Department of Computer Science, Code CS/Ic
	Naval Postgraduate School
	Monterey, California

	_____

14.	Mr. Daniel Warren, Department of Computer Science, Code CS/Wd
	Naval Postgraduate School
	Monterey, California

	_____

15.	Professor Tim Levin, Computer Science Department
	Naval Postgraduate School

	_____

16.	Mr. Emmett Henderson
	Naval Space Command

	_____

17.	Dr. Robert Ives, Department of Electrical and Computer Engineering
	Naval Postgraduate School

	_____

18.	Dr. Frank Kocher
	Oceanview Veterinarian Hospital

	_____

19.	Ms. Ann Jacobson, Code 013
	Naval Postgraduate School

	_____

20.	Ms. Kate McCrave, Code 013
	Naval Postgraduate School

	_____

21. Mr. Tommy Fifer, Code 34
Naval Postgraduate School

_____

22. Professor Dan Boger, Department of Information Systems
Naval Postgraduate School
Monterey, California

_____

23. Ms. Gail Thomas
Dell Corporation

_____

24. Ms. Letitia Haynes
Naval Postgraduate School